SUNGROW
Clean power for all

User Safety Operation Manual

Communication Module

WiFi-P2

Contents

All Rights Reserved

Sungrow Power Supply Co., Ltd.

Address: No. 1699, Xiyou Rd., High-tech Zone, Hefei City, Anhui Province, China

Zip code: 230088

Tel: 0551-6532 7878 / 0551-6532 7877

Official website: **www.sungrowpower.com**

1 About This Manual

This manual provides a detailed description of the security-related features of WiFi-P2 and specific operation instructions. For more information, visit **www.sungrowpower.com** or the website of the equipment manufacturer.

Scope of Application

This manual applies to the following devices:

- WiFi-P2

Product Model

Model	Product Aliases	Notes
WiFi-P2	Communication module	Supports WLAN

Target Group

This manual is intended for:

- Field maintenance personnel
- System administrator
- Field technical engineers

Manual Description

This manual uses the standard WiFi-P2 interface as an example to briefly introduce its safety and security functions. For specific supported functions, refer to the content of the technical agreement or the contract.

Security Disclaimer

To learn more about the product cybersecurity vulnerability disclosure and handling process, visit https://en.sungrowpower.com/security-vulnerability-management.

Symbols in the Manual

To ensure the safety of life and property for users when using the product and to improve the efficiency of product use, the manual provides relevant information, which is highlighted by the following symbols.

Symbols used in this manual are listed below. Please review carefully for better use of this manual.

⚠ DANGER

Indicates high-risk potential hazards that, if not avoided, may lead to death or serious injury.

⚠ WARNING

Indicates moderate-risk potential hazards that, if not avoided, may lead to death or serious injury.

⚠ CAUTION

Indicates low-risk potential hazards that, if not avoided, may lead to minor or moderate injury.

NOTICE

Indicates potential risks that, if not avoided, can lead to device malfunctions or financial losses.

Indicates additional information, emphasized contents, or tips that may be helpful, e.g. to help you solve problems or save time.

2 Basic Safety Instructions

⚠ WARNING

Life-threatening hazards caused by failure to follow safety instructions and risks from leftover components
Ignoring the safety instructions and the risks from leftover components in the attached hardware documentation may result in serious injury or death.

- **Follow the safety instructions in the hardware documentation.**
- **Consider the risks from leftover components during risk assessments.**

⚠ WARNING

Machine failures caused by incorrect parameter settings or modifications
Incorrect parameter settings may cause machine failures, resulting in serious injury or death.

- **Take protective measures to prevent unauthorized parameter settings.**
- **Take appropriate actions (such as stop or emergency stop) to handle potential faults.**

3 Cybersecurity Statement

Reverse Engineering Prohibition Statement

Reverse engineering, decompiling, disassembling, dismantling, modifying, implanting, or other derivative operations on the software product are prohibited. It is also prohibited to study the internal mechanisms of the product, obtain the source code, infringe on intellectual property rights, or disclose any software performance test results in any manner.

Privacy Statement

- To assist users with account registration, creation, and management, the system will collect the following information when creating a plant: retailer/installer email addresses, phone numbers (for China only), owner email addresses, and plant addresses. The above information is collected to provide better services and will not be used for any other purpose.
- When inverters, electricity meters, and other devices are connected to iSolarCloud, the system will collect the following information: inverter yield, real-time power of inverters, battery charge of hybrid inverters, battery discharge of hybrid inverters, forward active power of electricity meters, reverse active power of electricity meters, forward active kilowatt hours of electricity meters, and reverse active kilowatt hours of electricity meters. The above information is collected to help users monitor the operational status of their equipment and will not be used for any other purposes.
- When you use iSolarCloud to monitor and analyze the operational status of the plant, the system will collect the following information: plant name, plant type, plant status, installed capacity, real-time power, daily yield, device names, device status, fault names, fault occurrence time, and plant location. The above information is collected to help users manage the plant.

4 Potential Risks and Compensating Control Measures

Take the following compensating control measures to address potential risks:

Area	Issue	Risk	Compensating Control Measures
Security protocols	Insecure communication protocols are not allowed for transmitting encrypted data.	Malicious users may intercept communications if they gain network access.	For data transmission over internal networks, use physical or logical network segmentation. For data transmission over external networks, use virtual private networks (VPNs) or similar solutions to encrypt all protocol transmissions over external connections.

5 Security Hardening Guidelines

5.1 Port Matrix

This section describes the functions and default status of the product's service ports.

Port	Description
22	Used to connect to the server via Secure File Transfer Protocol (SFTP) for transferring data such as log files.
21	Used to connect to third-party devices via File Transfer Protocol (FTP). This port is disabled by default and is enabled only when required by the connected third-party device.
443	Used to connect to the local embedded Web or local App via Hypertext Transfer Protocol Secure (HTTPS).
67	Used to obtain IP addresses via Dynamic Host Configuration Protocol (DHCP).
5353	Used for fast network configuration via Multicast DNS (mDNS).
49152~65535	Used for the HTTP server to dynamically apply for a port for internal message communication.

5.2 External Interface Description

This section describes the external interfaces of the product.

Interface	Description
RJ45 connector	Used to power the communication module and for RS-485 communication.

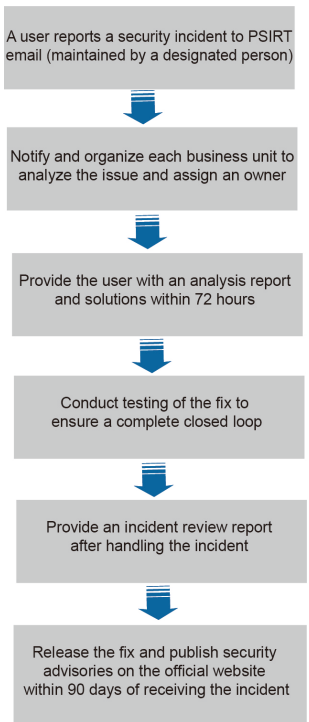
5.3 Instructions for Security-Related Functions

This section provides descriptions and recommendations for the following security-related functions and usage procedures:

Security Function	Description	Security Recommendations
User and password management	Password security policy configuration	Users change the default password upon first login, and it is recommended to update the password regularly and configure password security settings appropriately.
Protocol configuration	Configuration management of northbound protocols such as MQTT	It is recommended to enable protocols only as needed based on the minimization principle.
Certificate management and maintenance	HTTPS certificate management	It is recommended to update HTTPS certificates regularly.
Factory reset	Reset to factory settings and delete device data	It is recommended to use this function with caution.
System restoration	System restoration for devices malfunctioning after being attacked	Please contact SUNGROW Customer Service for restoration.
Security traceback	Operation log recording	It is recommended to analyze security logs regularly.
Security updates	Software and firmware updates	It is recommended to pay attention to product-related security announcements and update to the latest version in a timely manner.

5.4 Instructions for Reporting Product (Module) Security Incidents

The product security emergency response process is as follows:



If you discover a vulnerability in the product or a security risk in a module, click https://en.sungrowpower.com/security-vulnerability-management to visit the SUNGROW PSIRT page. On this page, you can click **More** to enter the details page, where you can view the list of security-related documents and vulnerability bulletins, or report security issues via email.

If the product security vulnerability has been fixed and a new version is available, you can update to the new version to fix the vulnerability on the **System > System Maintenance > System Update** page.

6 Account and Password Management

The administrator can assign different accounts and permissions to different users, which thus enhances the system security, improves operation efficiency for users, and lowers management costs. Three types of accounts are available in this system: General User, O&M User, and Developer. Their account names, default passwords, and permissions are as follows:

User Type	Account Name	Default Password	Permissions
General user	user	pw1111	Granted access to monitoring and general settings. For instance, Overview, Device monitoring, and some of the History data.
O&M user	admin	pw8888	Operations mentioned in this manual (except those requiring other specific permissions).
Developer	develop	Dynamically generated	Login with a developer account is allowed only after authorization by an O&M user account.

7 Guidelines for Safely Removing Products

The guidelines for safely removing reference and configuration data stored in the environment and safely removing the product are as follows:

- Before safely removing the product, refer to 8 Security Configuration Guide.
- To dispose of the device, refer to 8.4 Factory Reset and destroy it through safe channels to ensure that the device is not redeployed to the user's operational system or misused.

8 Security Configuration Guide

8.1 Deployment Security

This device is not a network device. To ensure the network security of the product and effectively prevent potential network risks, it is recommended to connect this device to a router with network traffic protection and control functions.

8.2 Password Management

Password Usage Security

- All passwords must meet strong complexity requirements. Change the default password upon first login.
- Change passwords promptly upon expiration.
- If you suspect a password has been compromised, change it immediately. Do not reuse old passwords. The system only checks whether the new password is identical to the old one. Do not use the same password across accounts.

8.3 Certificate Management and Maintenance

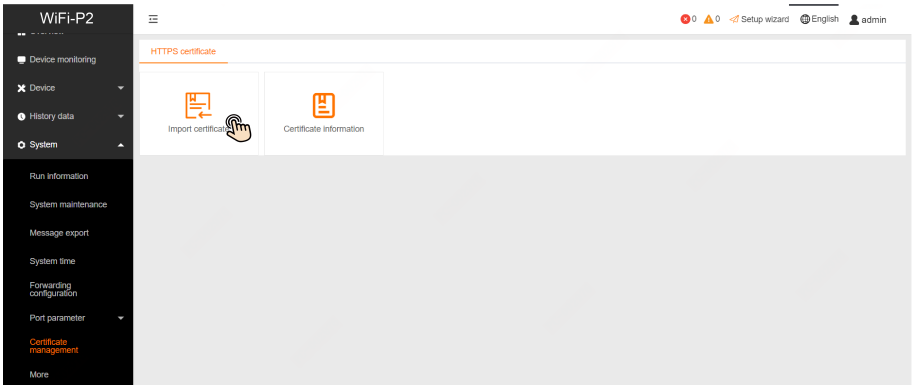
8.3.1 Pre-configured Certificate Risk Statement

Certificates are pre-configured on SUNGROW devices during the manufacturing process as their necessary identity credentials. Regarding the use of these pre-configured certificates, please note the following:

- Pre-configured certificates are only used to establish an initial secure channel for the device to access the customer network during the deployment process. SUNGROW does not promise or guarantee the security of the pre-configured certificates.
- SUNGROW does not promise or guarantee the security of the pre-configured certificates when used in services. It is recommended that users replace them with their own secure certificates.
- The validity period for the HTTPS and MQTT certificates pre-configured by SUNGROW is 30 years. Once a pre-configured certificate expires, the services that use this certificate remain available for communication.
- If users choose to use their own certificates, it is recommended that they properly manage the certificate lifecycle. Certificates with a short validity period are recommended to ensure security.

8.3.2 Certificate Security Maintenance

After logging in to the device, navigate to the **System > Certificate management** page and click **Import certificate** to import a certificate.



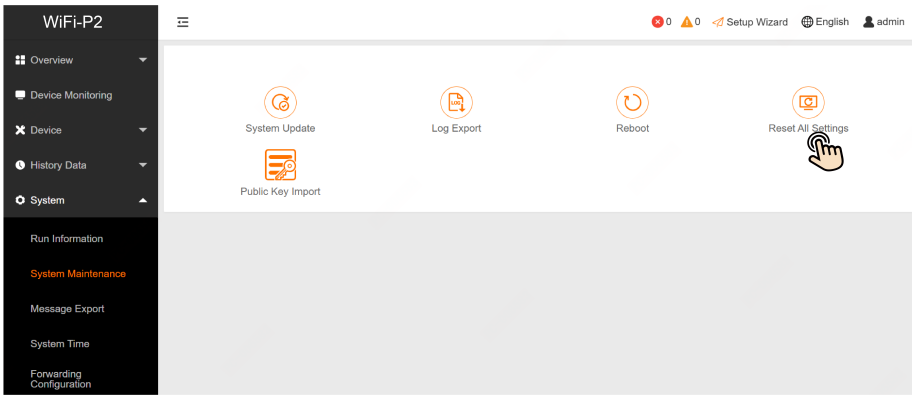
8.4 Factory Reset

If you suspect that the device is abnormal or its configuration has been maliciously tampered with, navigate to the **System > System maintenance** page and click **Reset all settings** to factory reset the device. The password will be reset to the default, and all history data will be deleted.

⚠ CAUTION

Please use the factory reset function with caution.

After a factory reset, the imported certificates will be invalid and replaced by the pre-configured certificates.



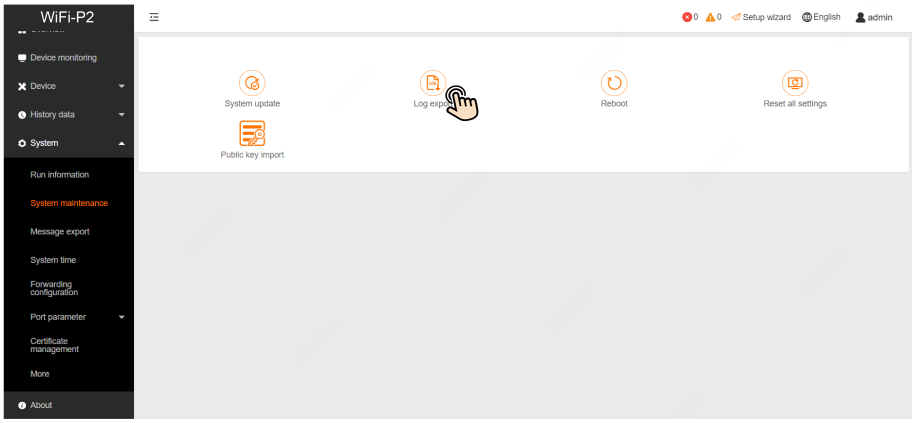
8.5 System Restoration

If the device has been attacked and cannot function properly, contact SUNGROW O&M personnel to replace the system through the UART port for restoration. The port is intended for qualified technical personnel only. To use the port, the device enclosure must be removed by using special tools.

The minimum system function that can work properly under an attack is to collect date from one device via the Modbus-RTU protocol.

8.6 Security Traceback

1. To review operations related to security incidents that have occurred, log in to the device, navigate to the **System > System maintenance** page, and click **Log export**.



2. You can also contact Sungrow O&M personnel to log in to the device's backend to assess the impact of the security incident and provide appropriate solutions.

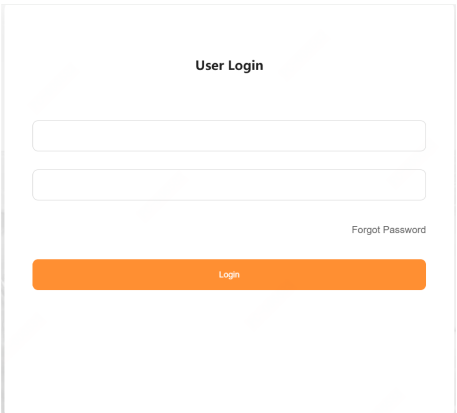
8.7 Security Updates

The term of software update commitment for this product is 5 years. You can perform secure version updates by verifying the digital signature of the update package, ensuring the integrity, authenticity, and confidentiality of the update package.

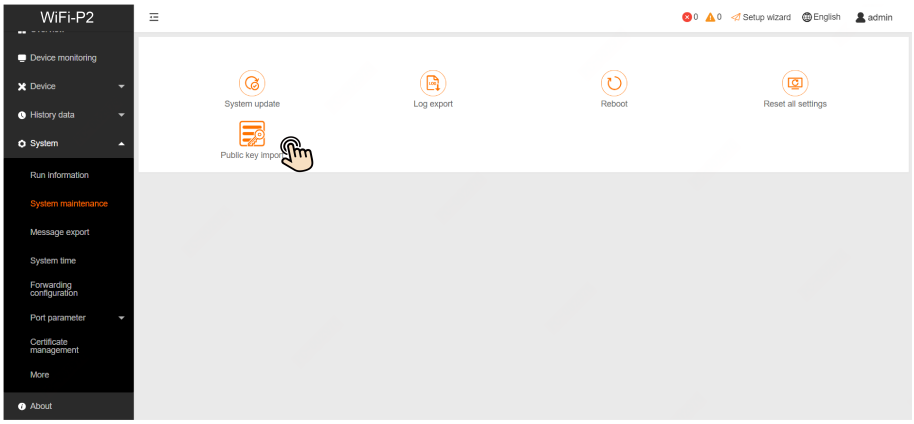
Security updates can be performed through the following methods: iSolarCloud App (remote), iSolarCloud App (local), iSolarCloud Web, local embedded Web, and the iConfig tool.

This manual provides instructions for a security update with the local embedded Web as an example.

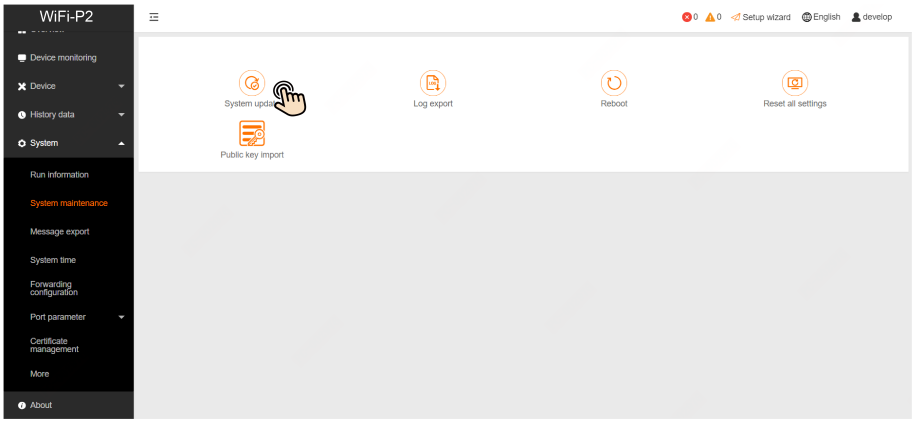
1. Log in to the local embedded Web.



2. Navigate to the **System > System maintenance** page and click **Public key import** to import a .pem public key file. (The public key is used to verify the digital signature of the update package. Perform this step if you need to update the public key file.)



3. Navigate to the **System > System maintenance** page and click **System update**. (The local update function is only supported under the develop account).



4. Select the update package to start the secure software update.

SUNGROW

Sungrow Power Supply Co., Ltd.

www.sungrowpower.com